Remote implementation of partially unknown operations and its entanglement costs

Shu-Hui Luo*,An-Min Wang†
Quantum Theory Group, Department of Modern Physics
University of Science and Technology of China, Hefei 230026, People Republic of China

We present the generalized version of Wang's protocol[A.M.Wang, Phys.Rev.A 74,032317 (2006)] for the remote implementation(sometimes referred to as quantum remote control) of partially unknown quantum operations. The protocol only requires no more than half of the entanglements used in Bidirectional Quantum State Teleportation. We also propose a protocol for another form of quantum remote control. It can remotely implement a unitary operation which is a combination of the projective representations of a group. Moreover, we prove that the Schmidt rank of the entanglements cannot not be less than the number of controlled parameters of the operations, which for the first time gives a lower bound on entanglement costs in remote implementation of quantum operations.

PACS numbers: 03.67.Lx

I. INTRODUCTION

In the construction of a quantum computer, it is difficult to maintain all qubits in a single processor due to decoherence. One alternative way is to build it as a multiprocessor device, that is to say, each processor contains only a few qubits. Evidently, such a "distributed quantum computer"[1] requires the remote implementation of quantum operations(RIO, sometimes also referred to as quantum remote control) since each processor can only perform limited local operations or it may not know all the information of the operations. Besides, RIO may also play important roles in distributed quantum computation, large scale quantum simulation, quantum programs or other remote quantum information processing tasks.

Without physically moving the qubits around, we can remotely implement operations using only local quantum operations and classical communications(LOCC) and prior entanglements. One straightforward way is resorting to Bidirectional Quantum State Teleportation(BQST)[2], where we teleport all the qubits involved to one party, and teleport them back after the desired operation is performed. And it is proved that when the operation is completely unknown, we can only rely on BQST [3]. BQST requires two rounds of teleportation. Indeed, it sets the upper bound on the resources needed for RIO.

As entanglements are valuable resources in quantum information and quantum computation, which are difficult to create and maintain, we should seek methods to save entanglements. Fortunately, when the operation falls into some restricted sets, we are able to remotely implement it using fewer entanglements via some protocols[4–7] than via BQST. Some experiments have been demonstrated[8, 9].

Reference [4] proposed the HPV protocol for quantum remote control of diagonal or anti-diagonal one-qubit operations. Reference [5] extended the HPV protocol to the Wang's protocol for the remote implementation of partially unknown multiqubits operations where there is only one nonzero element in every row or every column of the operations. By saying "partially unknown", we mean that Alice, the party that holds the quantum state to be operated on, does not know all the information of the remote operations. In the Wang's protocol, Alice only knows the structure of the operations, but not the nonzero elements of the operations. Reference [6] presented the protocols for combined and controlled remote implementations of partially unknown quantum operations of multiqubits using Greenberger-Horne-Zeilinger states. Reference [7] presented a hybrid protocol of remote implementations of quantum operations.

However, all the previous references did not give the minimum entanglement costs in RIO, even a lower bound. So we are curious about what is the necessary entanglement costs in RIO and whether there is a lower bound for entanglement costs in RIO. Recently we obtained a conclusion that the Schmidt rank(defined in [10]) of the entanglements cannot not be less than the number of controlled parameters of the operations, which for the first time provides a general lower bound on the required entanglement resource and gives a criterion to assess protocols for RIO. However, we haven't proved that the entanglement state should be maximally entangled, which we think should be the case.

Local implementation of nonlocal unitaries[11–14] is a different issue. In fact, there are profound connections

* lsh1990@mail.ustc.edu.cn
† amwang@ustc.edu.cn

between local implementation of nonlocal unitaries and RIO. Reference [14] proposed a protocol for implementing nonlocal controlled unitaries of the form $\mathcal{U} = \sum_{j=0}^{N-1} P_j \otimes V_j$ where the P_j's form a projective decomposition of the identity on $\mathcal{H}_A$, while the V_j's are arbitrary unitaries on $\mathcal{H}_B$. Reference [14] also presented a protocol for local implementation of nonlocal unitaries of the group decomposition form $\mathcal{U} = \sum_{f\in G} U(f) \otimes W(f)$ where the unitary operators $U(f)$'s form a finite-dimensional projective representation of a group G.

Inspired by Reference [5, 14], we figure out the generalized version of Wang's protocol[5] and a protocol for remote implementation of quantum operations which are combinations of the projective representations of groups. The former is able to remotely implement operations of the form

$$\mathcal{U} = \sum_{i=0}^{N-1} c_i A_i, \tag{1}$$

where c_i's are N arbitrary complex coefficients with modulus unity and A_i's satisfy $A_i^\dagger A_j = 0$, for $i \neq j$. The latter is able to remotely implement operations of the form

$$\mathcal{U} = \sum_{f\in G} c(f) U(f) \tag{2}$$

where the unitary operators $U(f)$'s form a finite-dimensional projective representation of a group G and $c(f)$'s are complex coefficients determined by $\mathcal{U}$.

Both of the protocols can remotely implement operations of certain forms using less entanglements than BQST. And they are indeed different kinds of quantum remote control. Previous protocols are quantum remote control similar to the generalized version of Wang's protocol. So it is worthwhile to present the Wang's protocol in a general way. But the protocol for RIO of group form is a different kind of quantum remote control. The form of remote operations it implements and the local operations it needs are different from those in the generalized version of Wang's protocol. Thus the protocol for RIO of group form is a good supplement to quantum remote control. There may still be other forms of quantum remote control. In a word, both the protocols we present in this paper would enhance the power of RIO and extend the applications of RIO.

The remainder of this paper is organized as follows. In Sec.II, we present the generalized version of Wang's protocol for RIO. Section III presents another protocol for RIO of the group form. Section IV proves that the Schmidt rank of entanglements cannot not be less than the number of controlled parameters of the operations. In Sec.V, we conclude our results.

II. A PROTOCOL OF RIO

Reference [4] presented a protocol for the remote implementation of quantum operations on a single qubit, where the operations are diagonal or anti-diagonal. Reference [5] presented the Wang's protocol for the remote implementation of partially unknown operations

$$U(x) = \sum_{i=0}^{2^N-1} e^{\mathrm{i}\phi_i} \left|p_i(x), D\right\rangle \left\langle i, D\right|, \tag{3}$$

on N qubits, where ϕ_i's are 2^N real phases and D indicates the decimal system, i.e., $|0, D\rangle = |00\ldots0\rangle, |1, D\rangle = |00\ldots1\rangle$, and $\left|2^N-1, D\right\rangle = |11\ldots1\rangle$, etc. $p(x) = \{p_0(x), p_1(x), \ldots, p_{2^N-1}(x)\}$ is a permutation of the list $\left\{0, 1, \ldots, 2^N-1\right\}$, where $x = 1, 2, \ldots, 2^N!$ maps all the permutations. This protocol uses N Bell states.

Now we present the generalized version of Wang's protocol for the remote implementation of operations in the form

$$\mathcal{U} = \sum_{i=0}^{N-1} c_i A_i \tag{4}$$

where c_i's are N arbitrary complex coefficients with modulus unity and A_i's satisfy $A_i^\dagger A_j = 0$, for $i \neq j$. Note that unlike the Wang's protocol, N here, the number of controlled parameters, has no relationship with the dimensionality of the Hilbert Space. Due to unitarity of $\mathcal{U}$, it can be proved that

$$A_i = \sum_{j=1}^{r_i} c_i |v_j^{(i)}\rangle\langle u_j^{(i)}| \tag{5}$$

where $\{|v_j\rangle\}$ and $\{|u_j\rangle\}$ are two full sets of mutually orthonormal vectors of the Hilbert Space and the superscript (i) indicates that a certain vector belongs to and only belongs to a certain A_i, so A_i's satisfy $A_i^\dagger A_j = 0$, for $i \neq j$. And r_i is the rank of A_i. The operations in Wang's protocol are special cases of this form when the ranks of A_i's equal to one.

We want to implement the operation on $\mathcal{H}_A$. Let the initial state of $\mathcal{H}_A$ be $|\Psi\rangle_A$. The entanglement resource is

$$|\Phi\rangle_{\rm ab} = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle \otimes |k\rangle, \tag{6}$$

where the dimension of $\mathcal{H}_a$ or $\mathcal{H}_b$ is N. For a given N define the X gate such that

$$X|k\rangle = |k-1\rangle. \tag{7}$$

Here, subtraction should be understood as mod N. The protocol has the following steps.

step 1 Alice performs

$$\mathcal{P} = \sum_{i=0}^{N-1} P_i \otimes X^i, \text{ where } P_i = \sum_{j=1}^{r_i} |u_j^{(i)}\rangle\langle u_j^{(i)}| \tag{8}$$

acts on $\mathcal{H}_A$, and X^i means X to the power i, which acts on $\mathcal{H}_a$. After this step the state of the combined system becomes

$$\sum_{i=0}^{N-1} P_i|\Psi\rangle_A \otimes \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k-i\rangle_a \otimes |k\rangle_b. \tag{9}$$

step 2 Alice performs a measurement on $\mathcal{H}_a$ in the computational basis. The measurement result l is sent to Bob. Bob then performs X^l on $\mathcal{H}_b$. The state of the system is now

$$\sum_{i=0}^{N-1} P_i|\Psi\rangle_A \otimes |i\rangle_b. \tag{10}$$

step 3 Bob performs $C = \sum_{i=0}^{N-1} c_i|i\rangle_b\langle i|$ on $\mathcal{H}_b$. The state of the system is

$$\sum_{i=0}^{N-1} c_i P_i|\Psi\rangle_A \otimes |i\rangle_b. \tag{11}$$

step 4 Bob performs a Fourier transform

$$F = \frac{1}{\sqrt{N}} \sum_{m,j=0}^{N-1} e^{2\pi {\rm imj}/N} |m\rangle\langle j| \tag{12}$$

on $\mathcal{H}_b$ and then measures $\mathcal{H}_b$ in the computational basis. The measurement result m is sent to Alice. The state of the system becomes

$$\sum_{j=0}^{N-1} e^{2\pi {\rm imj}/N} c_j P_j|\Psi\rangle_A \otimes |m\rangle_b. \tag{13}$$

step 5 Alice performs

$$\mathcal{R}_m = \sum_{j=0}^{N-1} \sum_{k=1}^{r_j} e^{-2\pi {\rm imj}/N} |v_k^{(j)}\rangle\langle u_k^{(j)}| \tag{14}$$

on $\mathcal{H}_A$. It completes the implementation of the operation. The final state is exactly

$$\mathcal{U}|\Psi\rangle_A = \sum_{j=0}^{N-1} c_j A_j|\Psi\rangle_A = \sum_{j=0}^{N-1} \sum_{k=1}^{r_j} c_j |v_k^{(j)}\rangle\langle u_k^{(j)}|\Psi\rangle_A. \tag{15}$$

It can be proved that operations of this form are all we can implement using such a protocol. Notice that c_i's can be chosen arbitrarily when A_i's are given. Besides, c_i's may be unknown to Alice, which keeps her from implementing the operation locally and obliges her to resort to RIO. Here lies the essence of quantum remote control[3, 4]. By such a protocol, Bob can apply a controlled and private operation on Alice's quantum state.

In fact, if Alice is able to locally implement any operation, by this protocol any unitary can be remotely implemented while Alice does not know all the information of the unitary. Because any unitary can be decomposed to a diagonal matrix with a unitary on each side by Singular Value Decomposition(SVD). For example $\mathcal{U} = \sum_{i=0}^{N-1} |u_i\rangle d_i \langle v_i| = \sum_{i=0}^{N-1} |u_i\rangle\langle i| \sum_{j=0}^{N-1} |j\rangle d_j \langle j| \sum_{k=0}^{N-1} |k\rangle\langle v_k| = udv$. If Bob wants to remotely implement a certain unitary $\mathcal{U}$ on Alice's quantum state while keeping Alice from knowing all the information of $\mathcal{U}$, he can first calculate the SVD of $\mathcal{U} = udv$ and tell Alice u and v. Then Alice performs v on her state. After that Bob remotely implements d using the above protocol. Finally Alice performs u. By this mean, $\mathcal{U}$ is remotely implemented while Alice does not know the elements of d. This method is nontrivial since if we use BQST instead, the entanglement costs would double.

But notice, in the above process Alice should have the devices to perform u and v. So if Alice and Bob want to remotely implement any unitary, Alice should have the devices to perform any local operation. Hence given limited devices, Alice and Bob can only remotely implement operations in some restricted sets. To enhance the power of RIO, we will present another protocol in the next section which can achieve a different form of RIO.

III. RIO OF GROUP FORM

Reference [14] presented a protocol for local implementation of nonlocal unitaries of the group decomposition form

$$\mathcal{U} = \sum_{f\in G} U(f) \otimes W(f) \tag{16}$$

where the unitary operators $U(f)$'s form a finite-dimensional projective representation of a group G. By saying projective representation, that means

$$U(f)U(g) = \mu(f,g)U(fg) \tag{17}$$

where $\mu(f,g)$'s are complex numbers constituting a factor system. Because of unitarity condition, $\mu(f,g)$'s are of modulus one. Using

$$U(g) = U(f^{-1})U(f)U(g) = \mu(f,g)U(f^{-1})U(fg) = \mu(f,g)\mu(f^{-1},fg)U(g), \tag{18}$$

we have $\mu(f,g)\mu(f^{-1},fg) = 1$. Hence, $\mu\left(h^{-1},f\right)\mu\left(h,h^{-1}f\right) = 1$. We will use this identity later.

In the following passages we will demonstrate the protocol to remotely implement operations of the form

$$\mathcal{U} = \sum_{f\in G} c(f)U(f) \tag{19}$$

where the unitary operators $U(f)$'s form a finite-dimensional projective representation of a group G and $c(f)$'s are controlled complex coefficients.

Before presenting the protocol, we first make some reasoning. The reasoning was motivated by the discussion in Part.II.B of Ref.[14]. Suppose we want to remotely implement an operation $\mathcal{U} = \sum_{i=0}^{N-1} c_i U_i$ on $\mathcal{H}_A$. And assume that the first two steps in Sec. II are necessary with P_i's being undefined. After the first two steps, we arrive at

$$\sum_{i=0}^{N-1} P_i|\Psi\rangle_A \otimes |i\rangle_b. \tag{20}$$

Then Bob performs an operation M on $\mathcal{H}_b$ and then measures $\mathcal{H}_b$ in the computational basis. The measurement result m is sent to Alice. Alice then performs a corresponding recovery operation $\mathcal{R}_m$ on $\mathcal{H}_A$. The final state of the system becomes

$$\sum_{i=0}^{N-1} \langle m|M|i\rangle R_m P_i|\Psi\rangle_A \otimes |m\rangle_b. \tag{21}$$

So if

$$\sum_{i=0}^{N-1} \langle m|M|i\rangle R_m P_i = \sum_{i=0}^{N-1} c_i U_i, \tag{22}$$

we have successfully applied the operation.

Particularly, define

$$U_i = U\left(g_i\right), R_m = U\left(g_m^{-1}\right), P_i = U\left(g_i\right), \langle m|M|i\rangle = \mu\left(g_m^{-1}, g_i\right)^{-1} c\left(g_m^{-1} g_i\right) \tag{23}$$

where g_i's are elements of a group G labeled by i and $U(g_i)$'s are their projective representations. Thanks to the Rearrangement Theorem in group theory,

$$\sum_{i=0}^{N-1} c\left(g_m^{-1} g_i\right) U\left(g_m^{-1} g_i\right) = \sum_{i=0}^{N-1} c\left(g_i\right) U\left(g_i\right). \tag{24}$$

Thus, we can successfully implement $\mathcal{U}$ by defining the operations as above.

The protocol follows from five steps.

step 1 Alice performs $\mathcal{P} = \sum_{f\in G} U(f) \otimes |f\rangle_a\langle f|$ where $|f\rangle_a$ are orthonormal basis on $\mathcal{H}_a$. After this step the state of the combined system becomes

$$\frac{1}{\sqrt{|G|}} \sum_{f\in G} U(f)|\Psi\rangle_A \otimes |f\rangle_a|f\rangle_b. \tag{25}$$

step 2 Alice performs F on $\mathcal{H}_a$ and then makes a measurement. The measurement result g is sent to Bob. The state of the system is

$$\sum_{f\in G} U(f)|\Psi\rangle_A \otimes \langle g|F|f\rangle|g\rangle_a|f\rangle_b. \tag{26}$$

step 3 Bob then performs $Z(g)$ on $\mathcal{H}_b$. $Z(g)$ is defined as

$$Z(g)|f\rangle = \frac{1}{\sqrt{|G|}}\langle g|F|f\rangle^{-1}|f\rangle. \tag{27}$$

The state of the system is now

$$\frac{1}{\sqrt{|G|}} \sum_{f\in G} U(f)|\Psi\rangle_A \otimes |g\rangle_a|f\rangle_b. \tag{28}$$

step 4 Bob performs M on $\mathcal{H}_b$. M is defined as

$$M = \sum_{f\in G} c(f)R(f), R(f) = \sum_{g\in G} \mu(g,f)|g\rangle\langle gf|. \tag{29}$$

Then Bob performs a measurement on $\mathcal{H}_b$. The measurement result h is sent to Alice. The state of the system becomes

$$\sum_{f\in G} U(f)|\Psi\rangle_A \otimes c\left(h^{-1}f\right)\mu\left(h, h^{-1}f\right)|g\rangle_a|h\rangle_b. \tag{30}$$

step 5 Alice performs $U(h^{-1})$ on $\mathcal{H}_A$. This completes the protocol. With $\mu\left(h^{-1}, f\right)\mu\left(h, h^{-1}f\right) = 1$, we arrive at

$$\mathcal{U}|\Psi\rangle_A \otimes |g\rangle_a|h\rangle_b = \sum_{f\in G} c(f)U(f)|\Psi\rangle_A \otimes |g\rangle_a|h\rangle_b. \tag{31}$$

It is easy to prove that this protocol is as general as BQST. The proof is similar to that in Part.V.A of Ref.[14]. And for a given projective representation of G and a given $\mathcal{U}$, $c(f)$'s are determined as

$$c(f) = \sum_{\lambda=1}^{\kappa} \frac{d_\lambda}{N} \sum_{j,k=1}^{d_\lambda} \left[D_{\mathrm{jk}}^{(\lambda)}(f)\right]^* \mathcal{R}_{\mathrm{jk}}^{(\lambda)} \tag{32}$$

where the notation is similar to that in Part.IV.D of Ref.[14]. For a given group, there are κ inequivalent unitary irreducible representations $\{D^{(\lambda)}(f)\}$ labeled by λ, where $D^{(\lambda)}(f)$ is a $d_\lambda \times d_\lambda$ matrix. And $\sum_{\lambda=1}^{\kappa} d_\lambda^2 = |G| = N$. In a certain basis of $\mathcal{H}_A$, $U(f)$ can be expressed in a block diagonal form

$$U(f) = \bigoplus_{\lambda=1}^{\kappa} D^{(\lambda)}(f). \tag{33}$$

Thus in that basis, $\mathcal{U}$ can also be expressed in a block diagonal form

$$\mathcal{U} = \sum_{f\in G} c(f)U(f) = \bigoplus_{\lambda=1}^{\kappa} \mathcal{R}^{(\lambda)}. \tag{34}$$

For simplicity, we are only talking in the situation in which the representation $U(f)$ contains each inequivalent irreducible representation exactly once. Please refer to Part.IV.C of Ref.[14] for further discussions. As the Double Unitary protocol in Part.IV.D of Ref.[14] is valid, our protocol is valid either.

Last but not least, Alice only needs the devices to perform $\mathcal{P}$, F and $U(f)$'s in the protocol. Given these devices, any combination of $U(f)$'s can be remotely implemented as long as the operation is unitary.

IV. ENTANGLEMENT COSTS

Alice has no information of c_i's. Hence, the information should be transmitted from Bob to Alice. By what means? Entanglements. A_i's and c_i's are coupled with the aid of entanglements.

For heuristic reason, first go through the protocol in Sec.II. We will use a diagrammatic method[15] to express the process.

Let the initial state of the system be $|\Psi\rangle_A \otimes \sum_{i=0}^{2} \frac{1}{\sqrt{3}}|i\rangle_a|i\rangle_b$. With the notation in Part.II.B of Ref.[14], it can be expressed as such a matrix:

a\b	0	1	2
0	$\frac{1}{\sqrt{3}}\|\Psi\rangle_A$	0	0
1	0	$\frac{1}{\sqrt{3}}\|\Psi\rangle_A$	0
2	0	0	$\frac{1}{\sqrt{3}}\|\Psi\rangle_A$

Here, the state of $\mathcal{H}_a$ is expressed as a column and the state of $\mathcal{H}_b$ is expressed as a row.

We want to implement

$$\mathcal{U}|\Psi\rangle = \sum_{i=0}^{2}\sum_{j=1}^{r_i} c_i|v_j^{(i)}\rangle\langle u_j^{(i)}|\Psi\rangle = \sum_{i=0}^{2} c_i A_i|\Psi\rangle_A = \begin{pmatrix} A_0 & A_1 & A_2 \end{pmatrix} \begin{pmatrix} |\Psi\rangle_A & & \\ & |\Psi\rangle_A & \\ & & |\Psi\rangle_A \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix}. \tag{35}$$

step 1 Alice performs

$$\mathcal{P} = \sum_{i=0}^{2} P_i \otimes X^i = \begin{pmatrix} P_0 & P_1 & P_2 \\ P_2 & P_0 & P_1 \\ P_1 & P_2 & P_0 \end{pmatrix}, \text{ where } P_i = \sum_{j=1}^{r_i} |u_j^{(i)}\rangle\langle u_j^{(i)}|. \tag{36}$$

After this step the state of the combined system becomes

$$\sum_{i=0}^{2} P_i|\Psi\rangle_A \otimes \frac{1}{\sqrt{3}}\sum_{k=0}^{2}|k-i\rangle_a \otimes |k\rangle_b = \frac{1}{\sqrt{3}} \begin{pmatrix} P_0|\Psi\rangle_A & P_1|\Psi\rangle_A & P_2|\Psi\rangle_A \\ P_2|\Psi\rangle_A & P_0|\Psi\rangle_A & P_1|\Psi\rangle_A \\ P_1|\Psi\rangle_A & P_2|\Psi\rangle_A & P_0|\Psi\rangle_A \end{pmatrix}. \tag{37}$$

step 2 Alice performs a measurement on $\mathcal{H}_a$ in the computational basis. The measurement result $l=1$ is sent to Bob. Bob then performs X on $\mathcal{H}_b$. The state of the system is now

$$\left(\begin{array}{ccc} P_2|\Psi\rangle_A & P_0|\Psi\rangle_A & P_1|\Psi\rangle_A \end{array} \right) \left(\begin{array}{ccc} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{array} \right) = \left(\begin{array}{ccc} P_0|\Psi\rangle_A & P_1|\Psi\rangle_A & P_2|\Psi\rangle_A \end{array} \right). \tag{38}$$

Because the state of $\mathcal{H}_b$ is expressed as a row, we use the transpose form of X. And we multiply $\sqrt{3}$ to preserve unitarity after performing a measurement.

step 3 Bob performs

$$C = \sum_{i=0}^{2} c_i |i\rangle_b\langle i| = \left(\begin{array}{ccc} c_0 & & \\ & c_1 & \\ & & c_2 \end{array} \right) \tag{39}$$

on $\mathcal{H}_b$. The state of the system is

$$\sum_{i=0}^{2} c_i P_i|\Psi\rangle_A \otimes |i\rangle_b = \left(\begin{array}{ccc} c_0P_0|\Psi\rangle_A & c_1P_1|\Psi\rangle_A & c_2P_2|\Psi\rangle_A \end{array} \right). \tag{40}$$

step 4 Bob performs a Fourier transform

$$F = \frac{1}{\sqrt{3}} \sum_{m,j=0}^{2} e^{2\pi \mathrm{imj}/3} |m\rangle\langle j| = \frac{1}{\sqrt{3}} \left(\begin{array}{ccc} 1 & 1 & 1 \\ 1 & e^{\frac{2\pi \mathrm{i}}{3}} & e^{\frac{4\pi \mathrm{i}}{3}} \\ 1 & e^{\frac{4\pi \mathrm{i}}{3}} & e^{\frac{8\pi \mathrm{i}}{3}} \end{array} \right) \tag{41}$$

on $\mathcal{H}_b$.

$$\sum_{i=0}^{2} c_i P_i|\Psi\rangle_A \otimes F|i\rangle_b = \left(\begin{array}{ccc} c_0P_0|\Psi\rangle_A & c_1P_1|\Psi\rangle_A & c_2P_2|\Psi\rangle_A \end{array} \right) \frac{1}{\sqrt{3}} \left(\begin{array}{ccc} 1 & 1 & 1 \\ 1 & e^{\frac{2\pi \mathrm{i}}{3}} & e^{\frac{4\pi \mathrm{i}}{3}} \\ 1 & e^{\frac{4\pi \mathrm{i}}{3}} & e^{\frac{8\pi \mathrm{i}}{3}} \end{array} \right) \tag{42}$$

Then measures $\mathcal{H}_b$ in the computational basis. The measurement result $m=2$ is sent to Alice. The state of the system becomes

$$\sum_{j=0}^{2} e^{4\pi \mathrm{ij}/3} c_j P_j|\Psi\rangle_A = c_0P_0|\Psi\rangle_A + e^{\frac{4\pi \mathrm{i}}{3}} c_1P_1|\Psi\rangle_A + e^{\frac{8\pi \mathrm{i}}{3}} c_2P_2|\Psi\rangle_A. \tag{43}$$

step 5 Alice performs

$$\mathcal{R}_m = \sum_{j=0}^{2} \sum_{k=1}^{r_j} e^{-2\pi \mathrm{imj}/3} |v_k^{(j)}\rangle\langle u_k^{(j)}| \tag{44}$$

on $\mathcal{H}_A$. It completes the remote implementation of the operation. The final state is exactly

$$\mathcal{U}|\Psi\rangle_A = \sum_{i=0}^{2} c_i A_i|\Psi\rangle_A = \sum_{i=0}^{2} \sum_{j=1}^{r_i} c_i |v_j^{(i)}\rangle\langle u_j^{(i)}|\Psi\rangle_A. \tag{45}$$

Indeed, the implementation can be summarized as follows. Assume that the measurement result of $\mathcal{H}_a$ is l and that of $\mathcal{H}_b$ is m. Obviously, Bob's action is subject to l. And the consequence of the measurement on $\mathcal{H}_a$ is to pick a row out of Alice's operation matrix, let it be $[\mathcal{P}_{ij}]$, while the consequence of the measurement on $\mathcal{H}_b$ is to pick a column out of Bob's operation matrix, let it be $[M_{ij}^{(l)}]^T$. In the end, Alice performs a recovery operation $\mathcal{R}_m$ on $\mathcal{H}_A$. The whole processing can be expressed as

$$\mathcal{U}|\Psi\rangle_A = \sqrt{n}\mathcal{R}_m \left(\begin{array}{cccc} \mathcal{P}_{l0} & \mathcal{P}_{l1} & \cdots & \mathcal{P}_{l(n-1)} \end{array} \right) \left(\begin{array}{cccc} |\Psi\rangle_A & 0 & \cdots & 0 \\ 0 & |\Psi\rangle_A & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & |\Psi\rangle_A \end{array} \right) \left(\begin{array}{c} {M^{(l)}}_{m0} \\ {M^{(l)}}_{m1} \\ \vdots \\ {M^{(l)}}_{m(n-1)} \end{array} \right)$$

$$= \begin{pmatrix} A_0 & A_1 & \cdots & A_{n-1} \end{pmatrix} \begin{pmatrix} |\Psi\rangle_A & 0 & \cdots & 0 \\ 0 & |\Psi\rangle_A & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & |\Psi\rangle_A \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix}. \tag{46}$$

Note, here the dimensionality of $\mathcal{H}_a$ or $\mathcal{H}_b$, or the Schmidt rank of entanglements, is equal to n, the number of c_i's, the controlled parameters. And the entanglement state is maximally entangled. Is it possible that d, the dimensionality of $\mathcal{H}_a$ or $\mathcal{H}_b$, is smaller than n? Or is it possible that the entanglement state is partially entangled?

Suppose it is possible. The entanglement state is $\sum_{i=0}^{d-1} \frac{1}{\sqrt{d}} h_i |i\rangle_a |i\rangle_b$(With Schmidt decomposition, we can always expressed entangled state in a diagonal form in a suitable basis). We have

$$\mathcal{U}|\Psi\rangle_A = \sum_{i=0}^{n-1} c_i A_i = \sqrt{d}\mathcal{R}_m \sum_{j=0}^{d-1} h_j {M^{(l)}}_{mj} \mathcal{P}_{lj}. \tag{47}$$

Since Alice has no knowledge of c_i's, when c_i's change and A_i's remain the same, Alice's action on $\mathcal{H}_A$, $\mathcal{P}$, should stay the same. Because c_i's are n arbitrary phase factors of modulus unity, their degree of freedom is n. When c_i's change and A_i's and $\mathcal{P}$ remain the same, the equation always holds. Thus, ${M^{(l)}}_{mj}$'s should be some linear combinations of c_i's. Just define

$${M^{(l)}}_{mj} = \sum_{i=0}^{n-1} {q^{(lm)}}_{ji} c_i. \tag{48}$$

Then we find

$$A_i = \sqrt{d}\mathcal{R}_m \sum_{j=0}^{d-1} h_j {q^{(lm)}}_{ji} \mathcal{P}_{lj}. \tag{49}$$

$\mathcal{P}_{lj} (j = 0, 1, \cdots, d-1)$ are at most d linearly independent operators. From (49), we can see A_i's are at most d linearly independent operators either because the rank of $[h_j {q^{(lm)}}_{ji}]$ may not exceed d. However, A_i's are n linearly independent operators by definition. So we come to the conclusion that the dimensionality of the entanglement resource, or the Schmidt rank of entanglements, cannot be smaller than the number of c_i's, the controlled parameters.

However, we are still unable to answer whether the entanglement resource should be maximally entangled. We believe the answer is yes.

Though the coefficients $c(f)$'s in the protocol of Sec.III are subject to (32), it can be easily proved that their degree of freedom is also equal to $|G|$, the number of elements in the group, since n^2 real parameters are needed to determine an $n \times n$ unitary matrix. We can prove that the Schmidt rank of entanglements required by that protocol cannot be less than $|G|$ similarly.

V. CONCLUSION

We present the generalized Wang's protocol for the remote implementation(remote control) of partially unknown quantum operations. We also propose the quantum remote control of group form. The protocols enhance the power of RIO and extend the applications of RIO. Then we prove that the Schmidt rank of the entanglement state cannot be less than the number of controlled parameters, which provides a lower bound for entanglement costs in RIO. But we are still unable to prove that the entanglement resource should be maximally entangled while previous protocols all require a maximally entangled state. This will be left for future study.

Our work analyzes the protocols for remote implementation of partially unknown quantum operations in detail and will provide some clues for new protocols, such as protocols for other forms of quantum remote control. Our work gives the necessary Schmidt rank of the entanglement resource for the first time. It provides clues for the minimum entanglement costs for RIO and gives a standard to evaluate previous protocols or future protocols. Since RIO has important applications in Quantum Information and Quantum Computation, our results are nontrivial. Future study should be cast to proposing protocols for other forms of quantum remote control and giving its minimum entanglement costs.

ACKNOWLEDGEMENTS

This work was supported by the National Natural Science Foundation of China under Grant No 10975125.

[1] J. Cirac, A. Ekert, S. Huelga, and C. Macchiavello, Physical Review A **59**, 4249 (1999).
[2] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Physical Review Letters **70**, 1895 (1993).
[3] S. Huelga, J. Vaccaro, A. Chefles, and M. Plenio, Physical Review A **63**, 042303 (2001).
[4] S. Huelga, M. Plenio, and J. Vaccaro, Physical Review A **65**, 042316 (2002).
[5] A.-M. Wang, Physical Review A **74**, 032317 (2006).
[6] A.-M. Wang, Physical Review A **75**, 062323 (2007).
[7] N.-B. Zhao and A.-M. Wang, Physical Review A **76**, 062317 (2007).
[8] G.-Y. Xiang, J. Li, and G.-C. Guo, Physical Review A **71**, 044304 (2005).
[9] S. F. Huelga, M. B. Plenio, G.-y. Xiang, J. Li, and G.-c. Guo, Journal of Optics B: Quantum and Semiclassical Optics **7**, S384 (2005).
[10] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).
[11] J. Eisert, K. Jacobs, P. Papadopoulos, and M. Plenio, Physical Review A **62**, 052317 (2000).
[12] Y. Huang, X. Ren, Y. Zhang, L. Duan, and G. Guo, Physical review letters **93**, 240501 (2004).
[13] N.-B. Zhao and A.-M. Wang, Physical Review A **78**, 014305 (2008).
[14] L. Yu, R. Griffiths, and S. Cohen, Physical Review A **81**, 062315 (2010).
[15] S. M. Cohen, "Visualizing Teleportation," (2007), eprint, arXiv:0704.0051 .